xahive

Your Cybersecurity Partner

XAHIVE’s Employee Security Checklist

□ Does your Board and C-Suite inform you regularly about current cyber threats and cyber issues and do they make you aware of these concerns for your organization?

□ Do you periodically review your org chart and who still has access to emails and other sensitive data?

□ Do you have an up to date research report concerning all operating systems, software applications and data center equipment operating within your data center?

□Do you periodically review the organization’s cybersecurity policies and procedures?

□ Do you evaluate the organization’s cybersecurity budget on a constant basis?

□ Do you have a recovery plan in place in case your data center or any other element of your IT infrastructure is compromised?

□ Do you have a clear image of the personnel, procedures and responsibilities (including systems and cross-functional training) involved in your infrastructure?

□ Does your organization have appropriate back up procedures in place to minimize downtime and prevent loss of important data?

□ Does your organization’s data center have adequate physical security controls to prevent unauthorized access?

□ Are there adequate environmental controls in place to ensure equipment is protected from fire and flooding?

□ Have you created and implemented the following cybersecurity policies?

- □ Acceptable Use Policy
- □ BYOD Policy
- □ Email and Communications Policy
- □ Encryption Policy
- □ Internet Access Policy
- □ Network Security Policy
- □ Privacy Policy
- □ Remote Access Policy

□ Is there a cybersecurity training program in place for current and new employees?

□ Do you have a list of the servers you use and is there a process in place ensuring that those servers are up to date?

□ Can that person investigate any anomalies that can potentially occur?

□ Do you have a patch management and or certification process for your servers and workstation used in your organization?

□ Do you have antivirus installed on your servers and workstations used in your organization?

□ Does your organization's server infrastructure have a host intrusion prevention solution or a firewall installed?

□ Do you periodically perform vulnerability scans on your servers and workstations used in your organization?

□ Do you use local encryption solutions for every workstation used in your organization?

□ Do you employ a password management system for your users?

□ Do you use wireless networks within your companies?

□ Are these wireless networks secured?

□ Do you have email filtering and Internet traffic filtering software that have the following capabilities: Protecting users from the full range of email threats, including malware, phishing and spam?

□ Do you have a solution that constantly scans for malware on your servers and workstations?

□ Do you have a clear protocol for file sharing? Do you have a process in place to protect documents and data stored in the cloud?

□ Is there a well-defined process for remote access and is this type of access properly secured?

□ Does your organization have a long-term plan concerning its cybersecurity strategy?

□ Do you have vigorously updated meta data and data mart analytics on what information your business stores and uses?

□ Have you developed a value associated with different types of data your organization transacts?

□ Have you conducted audits aimed at understanding your threats and vulnerabilities?

□ Are there policies to identify and control in place for staff, board and c-suite who have access to your business information?

□ Are new privileged users being subjected to background checks before being on boarded?

□ Do you require individual user accounts for each employee?

□ Are there policies and procedures for information security?

□ Do you limit employee access to data and information through role based controls?

□ Do you have Surge Protectors and Uninterruptible Power Supplies for your critical systems?

□ Do you regularly review CVEs and patch your operating systems and applications?

□ Does your organization use encryption for sensitive business information?

□ Is there a policy in place for disposing of old computers and media safely?

□ Is there a process in place to regularly train your employees?

□ Have you developed a plan for disasters and information security incidents?

□ Do you make full backups of important business data/information?

□ Have you considered cyber insurance?

□ Do you have a policy in place for regular review of the people you work with?

□Do you have a vendor information security policy in place?

□Do you certify your vendors for secure practices before engaging them?